

FILED  
LODGED  
ENTERED  
RECEIVED

AUG 02 2017

## UNITED STATES DISTRICT COURT

for the

Western District of Washington

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
DEPUTY  
BY

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)The business known as Bai Tong Thai Restaurant  
located at 14804 NE 24th Street  
Redmond, Washington 98052

Case No. MJ17-314

**Amended APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-2 (picture included with description), attached hereto and incorporated by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. § 371

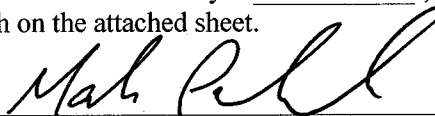
Offense Description  
Conspiracy to Commit Tax Evasion and Defraud the Government

The application is based on these facts:

See Affidavit of Special Agent Mark Pahnke, attached hereto and incorporated herein by reference.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

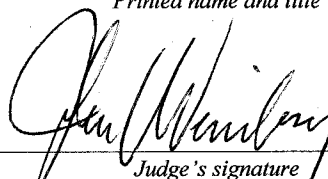
Mark Pahnke, Special Agent, IRS-CI

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/02/2017

City and state: Seattle, Washington



Judge's signature

John L. Weinberg, United States Magistrate Judge

Printed name and title

## **ATTACHMENT A2 – PREMISES TO BE SEARCHED**

This affidavit is made in support of an application for a warrant to search:

2. Bai Tong Thai Restaurant located at 14804 NE 24th St. Redmond, WA 98052.

The building is brown and has the name of the restaurant “Bai Tong Thai Restaurant” written above the main entrance. The number 14804 is written next to the front door.

The restaurant is located in a “stand alone” building located in a large parking lot. A picture of the restaurant is below:



## ATTACHMENT B - ITEMS TO BE SEIZED

The documents and records identified in this Attachment are evidence and/or instrumentalities of crimes against the United States, including Title 18 U.S.C. 371 (Conspiracy to commit tax evasion). For the period January 1, 2010 through the present, the following items, whether written, in original or reproduced format, or contained in computer sensitive media (as described in more detail in paragraph eight) or other format, including:

1. For PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA or their businesses<sup>1</sup>, evidence of business income and expenses such as receipt books, journals, ledgers, billing records and invoices, deposit slips, cancelled checks, bank statements, payroll records, significant amounts of cash, cash receipts, credit card receipts, home loan applications, deeds of trust, mortgage documents, cash expenses or receipts journals, worksheets, schedules and Quickbooks records.
2. For PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA or their businesses, income and expense records such as bank records, bank statements, deposit slips, wire transfers, other receipts showing evidence of money transfers, withdrawals or deposits. This can include receipts for cashier checks, money orders, financial statements, correspondence, investment accounts, accounting records, records of purchases and revenues received payroll records, income and informational tax returns, loan and mortgage records.
3. For PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA or their businesses, appointment schedule books or organizers, rolodex, client list, emails, contacts, vendor list, telephone numbers, personnel records and/or other items identifying clients or vendors or employees.
4. For PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA or their businesses, retained and draft copies of federal, state, and local tax returns, as well as

---

<sup>1</sup> For the purpose of this Search Warrant, PORNCHAI CHAISEEHA and CHADILLADA LAPANGKURA and their businesses shall be: Bai Tong Restaurant LLC, Bai Tong Family LLC, BT Capitol Hill LLC, Bai Tong Thai Corporation, Noi LLC, Noi Downtown Seattle LLC, Noi Hawaii LLC, and Isarn Soul Food LLC.

schedules, workpapers, documents, correspondence, and records used in the preparation of such forms.

5. For PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA or their businesses, any point of sale (POS) systems or records used to record, modify or delete revenues and/or expenses. Also any revenue suppression software (also known as Zapper software) or devices that house revenue suppression software, and any records that show sales, possession, or correspondence about revenue suppression software.

6. For PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA, any and all travel documents relating to travel, past or future, of PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA or their family members, including but not limited to PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA's United States passports and Thai passports.

7. For PORNCHAI CHAISEEHA, CHADILLADA LAPANGKURA or their businesses, the information described in paragraphs 1 through 6 may be contained, recorded or stored in or on Digital devices. "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players, or other electronic storage media. Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media, and/or their components, which include:

- a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;
- b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing

equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

h. Any digital devices or other electronic storage media that were or may have been used as a means to commit the offenses described on the warrant, including

i. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

j. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

k. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious

software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- l. evidence of the lack of such malicious software;
- m. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
- n. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
- o. evidence of the times the digital device or other electronic storage media was used;
- p. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;
- q. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;
- r. contextual information necessary to understand the evidence described in this attachment.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

SS

7

## 9

0

1

1 obtained from IRS computer databases, Washington State Department of Revenue (DOR)  
2 records, public records, surveillance observations and information obtained through other  
3 sources.

4 3. I have conducted and assisted in several investigations involving financial  
5 crimes. I have conducted search warrants and have interviewed witnesses and defendants  
6 who were involved in, or had knowledge of, violations of the Internal Revenue Code, the  
7 Bank Secrecy Act, and the Money Laundering Control Act. In the course of my employment  
8 with IRS-CI, I have conducted or been involved in investigations of these alleged criminal  
9 violations.

10 4. I make this affidavit in support of an application for a search warrant for the  
11 business and personal financial records. The two locations to be searched are described in  
12 the following paragraphs and in Attachments A1 and A2.

13 5. The facts set forth in this Affidavit are based on my own personal knowledge;  
14 knowledge obtained from other individuals during my participation in this investigation,  
15 including other law enforcement officers; review of documents and records related to this  
16 investigation; communications with others who have personal knowledge of the events and  
17 circumstances described herein; and information gained through my training and experience.  
18 Because this Affidavit is submitted for the limited purpose of establishing probable cause in  
19 support of the application for a search warrant, it does not set forth each and every fact that I  
20 or others have learned during the course of this investigation.

21 6. Based on my training and experience and the facts as set forth in this affidavit,  
22 there is probable cause to believe that the PORNCHEI CHAISEEHA, CHADILLADA  
23 LAPANGKURA, and BAI TONG GROUP, in collusion with SmilePOS, conspired to  
24 violate Title 18, United States Code, Section 371, Conspiracy to Commit Tax Evasion and  
25 Conspiracy to Defraud the United States. There is also probable cause to search the  
26 locations described in Attachments A1 and A2 for evidence, instrumentalities, contraband or  
27 fruits of these crimes further described in Attachment B.  
28



1 **II. SUMMARY OF REQUEST**

2  
3 7. I am currently conducting an investigation relating to PORNCHEI CHAISEEHA  
4 (CHAISEEHA) and CHADILLADA LAPANGKURA (LAPANGKURA), a married couple  
5 residing in Western Washington, and their businesses<sup>1</sup>. CHAISEEHA and LAPANGKURA  
6 are part owners in multiple Thai restaurants located in Washington, Oregon, and Hawaii. I  
7 am investigating the use of a Revenue Suppression Software (also known as Zapper  
8 Software) which I believe CHAISEEHA and LAPANGKURA use at their businesses in this  
9 district and elsewhere. Revenue Suppression Software (RSS) is software that interfaces with  
10 Accounting/Point of Sale software (such as SMILEPOS's software) to delete cash sales  
11 transactions from the system. The software automatically deletes the transactions and then  
12 reconciles the books of the business. The result is reconciled books and records that appear  
13 to be accurate but, in fact, show less than true income. These altered reports are presented to  
14 taxing authorities as genuine and therefore used to evade taxes. I make this Affidavit in  
15 support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a  
16 warrant to search a house and business (collectively "Search Locations") described below.  
17 As set forth in this Affidavit, there is probable cause to believe that evidence, fruits, and/or  
18 instrumentalities of a conspiracy to commit tax evasion and to defraud the government, in  
19 violation of Title 18, USC, Section 371, exist at the Search Locations.  
20

21 **III. LOCATIONS TO BE SEARCHED**

22 8. This Affidavit seeks authorization to search a residence ("Subject Premise) and  
23 business ("Subject Business") and any digital devices found therein. The Subject Premise is  
24 13921 SE 47<sup>th</sup> Street, Bellevue, Washington 98006. The Subject Business is 14804 NE 24th  
25 St. Redmond, Washington 98052.  
26

27 <sup>1</sup> For the purpose of this Search Warrant, PORNCHEI CHAISEEHA and CHADILLADA  
28 LAPANGKURA and their businesses shall be: Bai Tong Restaurant LLC, Bai Tong Family LLC, BT Capitol Hill  
LLC, Bai Tong Thai Corporation, Noi LLC, Noi Downtown Seattle LLC, Noi Hawaii LLC, and Isarn Soul Food LLC.

1           9.     The Subject Premise and Subject Business are more particularly described in  
2 Attachments A1 and A2 to this Affidavit, which is incorporated in full by this reference.  
3 “Digital device” includes any device capable of processing and/or storing data in electronic  
4 form, including, but input/output devices such as keyboards, printers, scanners, plotters,  
5 monitors, and drives intended for removable media, related communications devices such as  
6 modems, routers and switches, and electronic/digital security devices, wireless  
7 communication devices such as mobile or cellular telephones and telephone paging devices,  
8 personal data assistants (“PDAs”), iPods/iPads, Blackberries, digital cameras, digital gaming  
9 devices, global positioning satellite devices (GPS), or portable media players, not limited to:  
10 central processing units, laptop, desktop, notebook or tablet computers, computer servers, or  
11 peripherals.  
12

#### 13 **IV. FACTS ESTABLISHING PROBABLE CAUSE**

##### 14 ***Background***

15       10.     The restaurant industry has adopted modern technology to facilitate their point-  
16 of-sale (POS) transactions. These electronic POS systems keep track of dates/times,  
17 customers, servers, tables, orders, payments and refunds. Since all transactions are recorded  
18 in a database maintained by the POS software in real-time, database operations can be  
19 executed against the data to conveniently perform any type of calculation, e.g. to calculate  
20 monthly revenues. Tax collection agencies have granted businesses the option of  
21 predicated their tax burden on calculations derived from the electronic database maintained  
22 by the POS system with the stipulation that electronic sales data must be complete and must  
23 be furnished to the agencies on request in case of audit. This has effectively made obsolete  
24 the need to maintain physical receipts for tax purposes.

25       11.     While the use of electronic sales records as the basis for calculating taxes is  
26 convenient and cost-effective, the integrity of the system depends on comprehensive  
27 logging and immutability of the data. Each sales transaction must be assigned a unique  
28 transaction number that records the specifics of each transaction. The data is immutable,

1 i.e., it cannot be modified, so even if a sale is voided or a return is made, the original sales  
2 transaction is preserved and a new one is created to indicate the final outcome. Transaction  
3 numbers run consecutively with no gaps. In addition, all user and administrative functions  
4 must be logged.

5 12. The advent of electronic POS systems has heralded new techniques for tax  
6 evasion. Where in the past restaurants would keep two sets of books, one for reporting  
7 taxes and another with the actual figures, the reliance on electronic sales data has made the  
8 skimming of cash sales highly convenient using software tools.

9 13. Such tools are categorized as revenue suppression software (RSS) devices.  
10 RSS devices are software programs used to modify a business' POS database for the  
11 purpose of tax evasion by deleting or reducing sales transactions. Within this family is a  
12 subset called zappers. Unlike phantomware which is installed directly on the POS system  
13 computers and constantly run in the background, zappers are external programs that are  
14 executed at the time the deletions are to be made, typically from an external drive such as a  
15 flash drive.

16 14. In 2013, the State of Washington enacted Senate Bill 5715, codified at RCW  
17 82.32.290, which prohibits the possession, sale and use of automated sales suppression  
18 software (RSS, ESS or zappers). Scheduled as a Class C felony, Washington was the 14th  
19 state to pass legislation prohibiting the use of zappers.

## 20 21 **SMILEPOS**

### 22 *The Initial CI*

23 15. In October, 2015, I met with an HSI confidential informant (CI) to discuss a  
24 Lynnwood, Washington company named SmilePOS, LLC. This person has been a CI for  
25 over one year and in that time provided reliable information on another HSI investigation.  
26 He has one federal felony conviction relating to improper attempted export of firearm  
27 components.  
28

1       16.    The CI told us the following: Within the past year, he had worked at  
2 SmilePOS as an information technology (IT) support specialist and was responsible for the  
3 setup and deployment of POS systems to clients, as well as was tasked to provide technical  
4 support to the clients. During one customer support call, the customer requested support for  
5 a software application called "Freshbooks." The CI was unfamiliar with the application as it  
6 was not part of the official POS suite so he consulted Saksit Udompanit, Owner and Sales  
7 Manager of SmilePOS, about the application. Udompanit confided to the CI that  
8 "Freshbooks" is a software program used by clients to delete records of cash transactions  
9 from their electronic books in an undetectable manner. "Freshbooks" is an RSS or zapper  
10 program. Udompanit directed the CI to support the application and, further, to provide it to  
11 any client who requested it.

12       17.    The CI estimated that SmilePOS has up to 500 clients, a group almost entirely  
13 composed of Thai restaurants (the program is written in the Thai and English languages).  
14 Of those clients, the CI said he believes that a sizeable majority of them have "Freshbooks."  
15 Udompanit told the CI that customers demanded a way to easily conceal the deletion of cash  
16 transactions and would not have purchased SmilePOS if it lacked that feature.

17       18.    To corroborate his statements, the CI provided me a copy of SmilePOS and  
18 "Freshbooks" programs installed on a standalone computer and demonstrated how it worked.  
19 First, the CI started SmilePOS and created several example sales including one with some  
20 cash payments. For each sale, a corresponding ticket was created in the POS database and  
21 assigned a unique ticket identification number (ticketID). The ticketID was automatically  
22 generated to the next higher sequential number on the next ticket. For example, if the first  
23 ticketID was 201510230001, the next would be 201510230002, followed by 201510230003  
24 as shown in Figure 1.

25       *Figure 1.*

26           TicketID  
27           201510230001  
28           201510230002 [assume a cash sale]  
             201510230003  
             201510230004 [assume a cash sale]

1 201510230005

2  
3 19. With the tickets in the system, the CI demonstrated how "Freshbooks" was  
4 used. By selecting a specific date, the program would show all cash payment tickets made  
5 on that date (tickets 201510230002 and 201510230004) which the CI then deleted.  
6 Typically in a POS software program, a deleted ticket will result in a non-sequential gap in  
7 the ticketID sequence, as in Figure 2.

8 *Figure 2.*

9 TicketID

10 201510230001

11 201510230003

12 201510230005

*Tickets 2 and 4 are missing because they were cash sales which were deleted.*

13 20. The CI demonstrated how "Freshbooks" compensates for the ticketID gap. He  
14 deleted several cash sales tickets then showed us that the deleted tickets were also deleted  
15 from the database. The subsequent ticketIDs were renumbered to conceal the deletions, as  
16 shown in Figure 3.

17  
18 *Figure 3.*

19 TicketID (Before)

TicketID (After)

20 201510230001

201510230001

21 201510230003

→

201510230002

22 201510230005

→

201510230003

23 "Freshbooks" operates only on the SmilePOS system because it interacts with database  
24 tables which are unique to SmilePOS. The only reason a business uses "Freshbooks" to  
25 delete and renumber cash sales tickets is to hide cash sales and produce business records that  
26 appear legitimate. The primary reason to create false records is to evade state, local and  
27 federal taxes.

28 ***The Second CI***

1        21.    Later in 2015, we interviewed another employee of SmilePOS herein referred  
2 to as "CI 2." CI 2 is a Thai national with no known criminal history who currently resides in  
3 the United States. When we first met he was living in the United States after his visa had  
4 expired. Currently he is living in the United States on deferred action with a valid work  
5 authorization. CI 2 advised that he worked for SmilePOS for several years and is very  
6 familiar with the owner, Saksit Udompanit. In addition to corroborating the facts provided  
7 by the original CI, CI 2 provided the following additional information:

8        22.    Udompanit told CI 2 that he studied computer science and developed the initial  
9 version of the SmilePOS software. Udompanit created an LLC in the State of Washington  
10 called N-Tier Computer Solutions (N-Tier) and marketed SmilePOS to Thai restaurants.

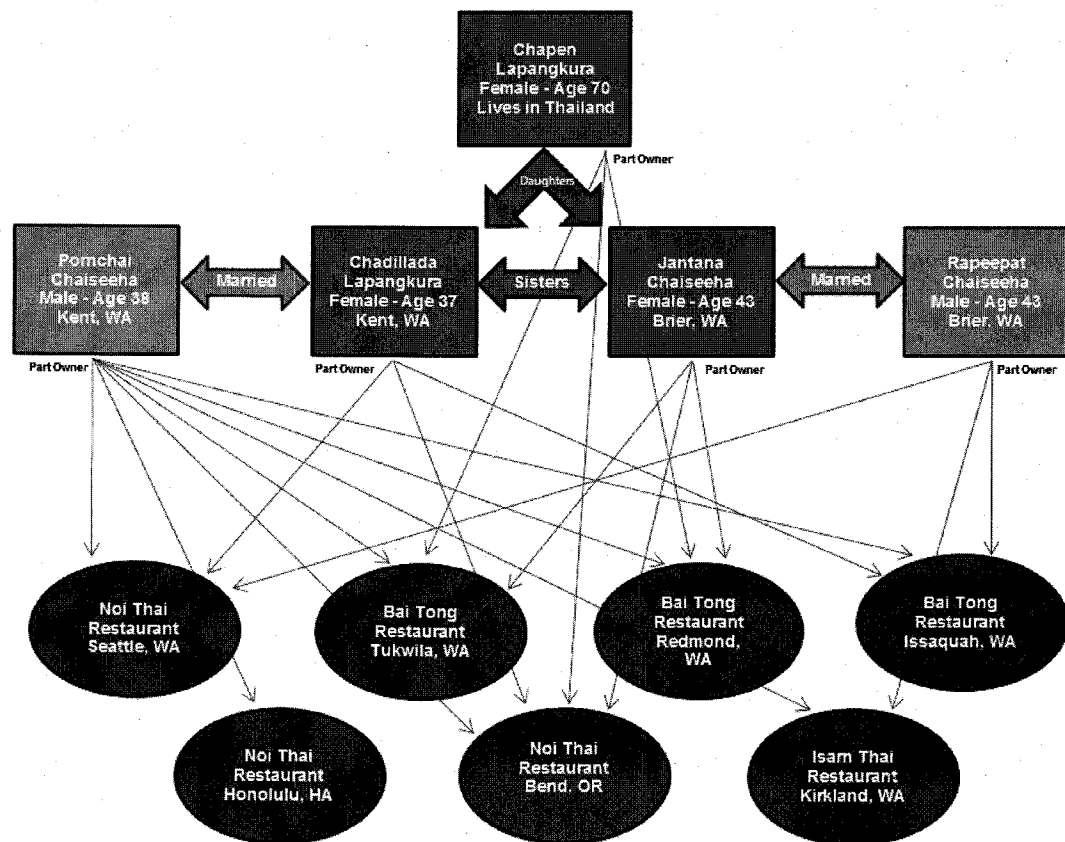
11       23.    As N-Tier grew, Udompanit recruited CI 2 to work with him. In 2015,  
12 Udompanit dissolved N-Tier and created a new Washington State LLC called SmilePOS.  
13 When CI 2 was brought on, Udompanit introduced to him to a zapper tool that Udompanit  
14 had developed in conjunction with the SmilePOS software. This zapper was called  
15 "ShowTicket" and its existence and purpose was an open secret within the company. Other  
16 employees were aware of the tool, especially sales personnel, since sales personnel provided  
17 training on the tool when clients purchased a POS system. Although sales personnel would  
18 provide the RSS or zapper to clients, IT personnel also were directed to provide the zapper to  
19 clients if they requested a new copy. IT personnel provided the zapper by uploading the  
20 executable file to the root directory of the clients' POS system C drive. Based on CI 2's  
21 interactions with clients he estimates that most of the client restaurants are using the zapper.  
22 He provided us with a list of the SmilePOS clients which included the Bai Tong Group  
23 restaurants which are partly owned by CHAISEEHA and LAPANGKURA.

24       24.    Within the past few years, "ShowTicket" was renamed "Freshbooks."  
25 Udompanit explained to CI 2 that he changed the name because a POS competitor in San  
26 Francisco "tried to get the company in trouble" with unnamed authorities so he felt the need  
27 to distance the company from the "ShowTicket" name.  
28

1           25.     I have learned that the State of California investigated possible use of RSS in  
2 several Thai restaurants beginning in 2013 and I believe this is what Udompanit referenced.  
3 In November 2015, I spoke with Warren Klomp (Klomp), lead of the POS Department of  
4 California's Board of Equalization (BOE). Klomp told me that BOE has been aware that  
5 SmilePOS, LLC had been selling RSS to clients in California for quite some time and that, in  
6 June 2013, his department received an anonymously sent package. The package contained  
7 the records of 11 restaurants that used SmilePOS computer systems. The package alleged  
8 that the restaurants were using the SmilePOS system to delete cash sales, generate and send  
9 false summary reports to BOE, and commit tax evasion. The package contained a summary  
10 sheet and before and after reports (i.e., a true report and an altered report) for specific time  
11 periods for each of the restaurants. After receiving this information BOE investigated further  
12 and found several SmilePOS clients had missing cash receipts in their databases.  
13

14 ***Introduction to PORNCHAI CHAISEEHA and the Bai Tong Group***

15           26.     The Bai Tong Group began with one restaurant in 1989, opened to serve Thai  
16 Airways crew on layovers in Seattle. Since then the Group has expanded to several  
17 restaurants, all Thai and operating under a variety of names, in Redmond, Tukwila, Issaquah,  
18 Kirkland, Lynnwood, Seattle, Honolulu and Bend, Oregon. According to Washington State  
19 corporate records and business news articles, the Bai Tong Group restaurants are owned and  
20 operated by the founder, Chanpen Lapangkura, her daughters and their husbands. There are  
21 also additional partners. Below is a diagram I have created based on IRS records and  
22 publicly available information:  
23  
24  
25  
26  
27  
28



#### ***DOR Audit of Bai Tong Restaurant in Redmond, Washington***


27. Bai Tong Thai Restaurant in Redmond, Washington is legally known as *Bai Tong Family LLC* and is registered with the Internal Revenue Service, the Washington Secretary of State, and the Washington State Department of Revenue. This particular Bai Tong restaurant is owned by Chanpen Lapangkura (50%), Pornchai Chaiseeha (25%) and Jantana Chaiseeha (25%).

28. On November 13, 2015, I spoke with Bryan Kelly (Kelly), Audit Project Manager for Washington State Department of Revenue (DOR). Kelly is in charge of DOR's audit team which has been investigating businesses suspected of using zipper to evade taxes. DOR has been investigating the possible use in Washington State for over few years. Kelly told me the following.



29. In in last several years DOR audited businesses that are known users of SmilePOS computer systems. In at least five of these audits Kelly's team suspected the businesses were using zappers with their SmilePOS systems to delete cash transactions, thereby avoiding state sales taxes on those transactions. Kelly's team suspected these businesses as the businesses reported substantially lower than expected cash sales. To investigate, DOR auditors made cash purchases at each of the restaurants before beginning the DOR audits. The auditors kept their cash receipts generated by the SmilePOS system.

30. A few months later, and during the DOR audits, the auditors requested the full SmilePOS database, including detailed transactions. Once received, the auditor would look in the database for the specific cash receipt from his/her purchase to determine whether that specific cash transaction was accounted for in the database or was deleted. Kelly identified Bai Tong Thai Restaurant located at 14804 NE 24th Street, Redmond, Washington, as one of the restaurants having deleted transactions in its SmilePOS database. The receipts here are two of the cash transactions which were not in the POS records supplied to DOR.


  
**BAI TONG**  
THAI RESTAURANT  
Bai Tong Thai Restaurant  
14804 NE 24th ST  
Redmond WA 98052  
Tel. 425.747.8424 Fax. 425.747.2345  
www.baitongrestaurant.com  
Hello, Thank You for Coming.

**Table A4**  
Date: 2/13/2014 7:06 PM  
Server: Mon (T.1)

Thai Iced Tea (28\$2.95)	\$5.90
Crispy Garlic Chicken	\$13.95
Asparagus Mushroom	\$11.95
Garlic Fish Fry	\$15.95
Pa-Nang Curry	\$10.95
Phad Thai (Prawns)	\$11.95
Kint Mao Noodles	\$10.95
Steamed Rice	\$1.50
Brown Rice (38\$2.00)	\$6.00
Total 12 item(s)	\$89.10
Gratuity	\$16.04
Sales Tax	\$9.99
<b>Grand Total</b>	<b>\$115.13</b>

18% Gratuity included for a party of 6 people or more.  
Thank you. Please Come Again.

- GUEST CHECK -

  
**BAI TONG**  
THAI RESTAURANT  
Bai Tong Thai Restaurant  
14804 NE 24th ST  
Redmond WA 98052  
Tel. 425.747.8424 Fax. 425.747.2345  
www.baitongrestaurant.com  
Hello, Thank You for Coming.

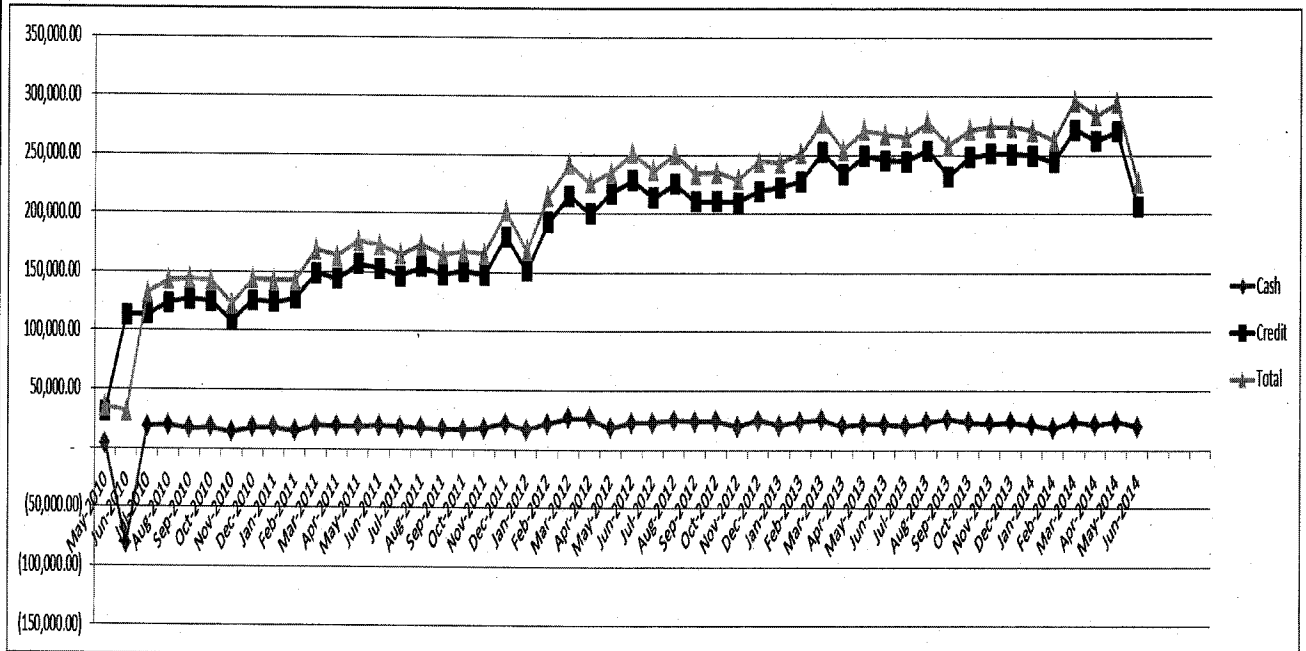
**Table A5**  
Date: 2/8/2014 7:17 PM  
Server: Nooch S (T.1)

Crispy Garlic Chicken	\$13.95
Kang Pa	\$10.95
Phad Thai	\$9.95
Brown Rice (28\$2.00)	\$4.00
Bai-Tong-Tina (28\$8.50)	\$17.00
Manny (28\$6.00)	\$12.00
Crab Wonton Small	\$5.50
Total 10 item(s)	\$73.35
Sales Tax	\$6.97
<b>Grand Total</b>	<b>\$80.32</b>

Tip Guide  
15%-\$12.05, 18%-\$14.46, 20%-\$16.06  
18% Gratuity included for a party of 6 people or more.  
Thank you. Please Come Again.

- GUEST CHECK -

31. Below is a line graph I made based on public filings and state tax returns filed with the Washington Department of Revenue. The graph illustrates the Redmond Bai Tong restaurant's reported sales data from May 2010 to June 2014 and shows cash sales and credit card sales. The reported data indicates that during the time period credit card sales increased dramatically while cash sales remained flat. This is a highly unusual pattern and more likely is a reflection of the use of zapper software than of actual flat cash sales.



32. For the years 2011 to 2014, I have compared the amount of revenue that Bai Tong Redmond reported to the State of Washington in their state tax returns to the amount of money that Bai Tong Redmond reported to the IRS on federal income tax returns. The gross revenue reported to both DOR and the IRS matches with less than 1% difference. Therefore, if Bai Tong Thai Restaurant in Redmond is under reporting revenue to Washington Department of Revenue they are also under reporting revenue to the I.R.S.

33. I estimate that within the time period reflected in the graph, this one restaurant defrauded Washington State and the Federal Governments of approximately \$371,870.00 in unpaid taxes.

1 ***Search Warrant Executed On SmilePOS Emails***

2 34. On December 21, 2015, a federal search warrant was signed for SmilePOS  
3 business emails. The data seized included emails between Bai Tong and SmilePOS,  
4 including one with this header:

5 **Subject:** Southcenter Bai Tong  
6 **From:** Baitong Thai <baitongrestaurant@hotmail.com>  
7 **Date:** 7/14/2012 12:25 AM  
8 **To:** Prem <saksit@smilepos.com>, SmilePOS Prem <support@smilepos.com>, Prem  
hotmail <premy19@hotmail.com>

9 The body of the email text is in Thai; the following is a translation.  
10

11 Hello Prem,  
12 I had a meeting today at the restaurant and they want help with something.

13 *[a section asking for assistance re: To Go orders]*

14 Another thing, I [Noi] can't get into the program show ticket at the South store;  
15 it tells me that not "connect to server".

16 Prem, can you please fix it?

17 Thank you very much, Noi  
18

19 35. We have learned that "Noi" is in the name of three of the restaurants and it is  
20 CHADILLADA LAPANGKURA'S nickname. Showticket is the name of the "Zapper"  
21 software.

22 36. Another email from LAPANGKURA Hotmail account to the technical support  
23 email account at SmilePOS references the zapper program and attached screen shots relating  
24 to the zapper program.  
25  
26  
27  
28

1  
2  
3 **Subject:** Showticket Noi

4 **From:** Chadillada Lapangkura <chadillada@hotmail.com>

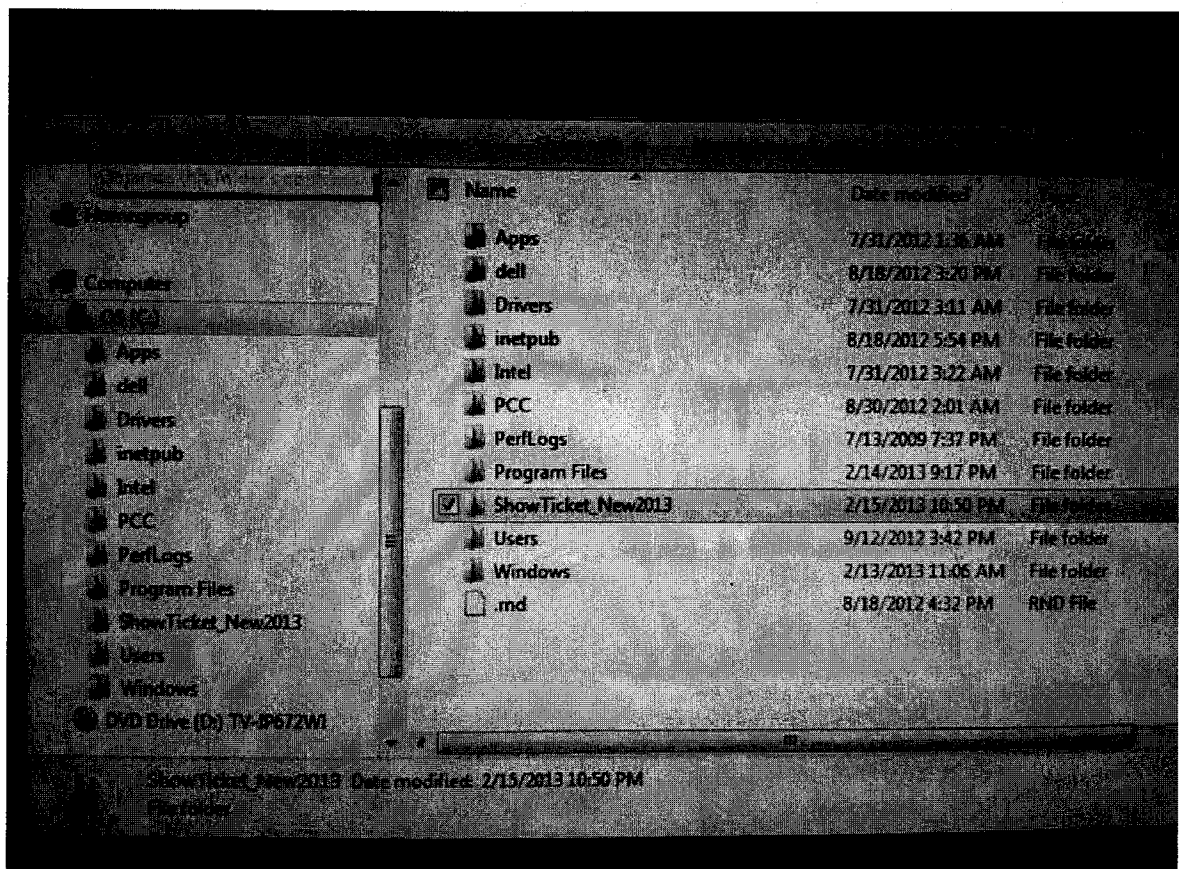
5 **Date:** 2/17/2013 9:55 PM

6 **To:** support@smilepos.com

7 Prem ka.

- 8
- 9 - new program is in Showticket new 2013 folder chai mai ka?
  - 10 - the main server is the one at host station?
  - 11 - can u check Jan 1,6,12 please? We adjusted these 3 days and there were something wrong. Sales (after adjustment) were higher than what we actually made.

12 Thank you ka.



Case No.	Amount	Date	Time	Balance
120182	1.3	1/1/2013 8:00 PM	Cash	87.00
120182	2.48	1/1/2013 8:00 PM	Cash	89.48
120182	4.32	1/1/2013 8:00 PM	Cash	93.80
120182	4.34	1/1/2013 8:00 PM	Cash	98.14
120182	7.35	1/1/2013 8:00 PM	Cash	105.49
120182	8.36	1/1/2013 8:00 PM	Cash	113.85
120182	9.37	1/1/2013 8:00 PM	Cash	123.22
120182	11.38	1/1/2013 8:00 PM	Cash	134.60
120182	12.39	1/1/2013 8:00 PM	Cash	146.99
120182	13.40	1/1/2013 8:00 PM	Cash	160.39
120182	14.41	1/1/2013 8:00 PM	Cash	174.80
120182	15.42	1/1/2013 8:00 PM	Cash	190.22
120182	16.43	1/1/2013 8:00 PM	Cash	206.65
120182	17.44	1/1/2013 8:00 PM	Cash	224.09
120182	18.45	1/1/2013 8:00 PM	Cash	242.54
120182	19.46	1/1/2013 8:00 PM	Cash	262.00
120182	20.47	1/1/2013 8:00 PM	Cash	282.47
120182	21.48	1/1/2013 8:00 PM	Cash	303.95
120182	22.49	1/1/2013 8:00 PM	Cash	326.44
120182	23.50	1/1/2013 8:00 PM	Cash	350.94
120182	24.51	1/1/2013 8:00 PM	Cash	376.45
120182	25.52	1/1/2013 8:00 PM	Cash	402.97
120182	26.53	1/1/2013 8:00 PM	Cash	430.50
120182	27.54	1/1/2013 8:00 PM	Cash	459.04
120182	28.55	1/1/2013 8:00 PM	Cash	488.59
120182	29.56	1/1/2013 8:00 PM	Cash	519.15
120182	30.57	1/1/2013 8:00 PM	Cash	550.72
120182	31.58	1/1/2013 8:00 PM	Cash	583.30
120182	32.59	1/1/2013 8:00 PM	Cash	616.89
Total				650.00

Case No.	Amount	Date	Time	Balance
120182	33.60	1/1/2013 8:00 PM	Cash	650.00
120182	34.61	1/1/2013 8:00 PM	Cash	684.61
120182	35.62	1/1/2013 8:00 PM	Cash	720.23
120182	36.63	1/1/2013 8:00 PM	Cash	756.86
120182	37.64	1/1/2013 8:00 PM	Cash	794.50
120182	38.65	1/1/2013 8:00 PM	Cash	833.15
120182	39.66	1/1/2013 8:00 PM	Cash	872.81
120182	40.67	1/1/2013 8:00 PM	Cash	913.48
120182	41.68	1/1/2013 8:00 PM	Cash	955.16
120182	42.69	1/1/2013 8:00 PM	Cash	997.85
120182	43.70	1/1/2013 8:00 PM	Cash	1041.55
120182	44.71	1/1/2013 8:00 PM	Cash	1086.26
120182	45.72	1/1/2013 8:00 PM	Cash	1132.00
120182	46.73	1/1/2013 8:00 PM	Cash	1178.73
120182	47.74	1/1/2013 8:00 PM	Cash	1226.47
120182	48.75	1/1/2013 8:00 PM	Cash	1275.22
120182	49.76	1/1/2013 8:00 PM	Cash	1325.00
120182	50.77	1/1/2013 8:00 PM	Cash	1375.77
120182	51.78	1/1/2013 8:00 PM	Cash	1427.55
120182	52.79	1/1/2013 8:00 PM	Cash	1480.34
120182	53.80	1/1/2013 8:00 PM	Cash	1534.14
120182	54.81	1/1/2013 8:00 PM	Cash	1588.95
120182	55.82	1/1/2013 8:00 PM	Cash	1644.77
120182	56.83	1/1/2013 8:00 PM	Cash	1701.60
120182	57.84	1/1/2013 8:00 PM	Cash	1759.44
120182	58.85	1/1/2013 8:00 PM	Cash	1818.29
120182	59.86	1/1/2013 8:00 PM	Cash	1878.15
120182	60.87	1/1/2013 8:00 PM	Cash	1939.02
120182	61.88	1/1/2013 8:00 PM	Cash	2000.90
120182	62.89	1/1/2013 8:00 PM	Cash	2063.79
120182	63.90	1/1/2013 8:00 PM	Cash	2127.69
120182	64.91	1/1/2013 8:00 PM	Cash	2192.60
120182	65.92	1/1/2013 8:00 PM	Cash	2258.52
120182	66.93	1/1/2013 8:00 PM	Cash	2325.45
120182	67.94	1/1/2013 8:00 PM	Cash	2393.39
120182	68.95	1/1/2013 8:00 PM	Cash	2462.34
120182	69.96	1/1/2013 8:00 PM	Cash	2532.30
120182	70.97	1/1/2013 8:00 PM	Cash	2603.27
120182	71.98	1/1/2013 8:00 PM	Cash	2675.25
120182	72.99	1/1/2013 8:00 PM	Cash	2748.24
120182	73.00	1/1/2013 8:00 PM	Cash	2822.24
120182	74.01	1/1/2013 8:00 PM	Cash	2897.25
120182	75.02	1/1/2013 8:00 PM	Cash	2973.27
120182	76.03	1/1/2013 8:00 PM	Cash	3050.30
120182	77.04	1/1/2013 8:00 PM	Cash	3128.34
120182	78.05	1/1/2013 8:00 PM	Cash	3207.39
120182	79.06	1/1/2013 8:00 PM	Cash	3287.45
120182	80.07	1/1/2013 8:00 PM	Cash	3368.52
120182	81.08	1/1/2013 8:00 PM	Cash	3450.60
120182	82.09	1/1/2013 8:00 PM	Cash	3533.69
120182	83.10	1/1/2013 8:00 PM	Cash	3617.79
120182	84.11	1/1/2013 8:00 PM	Cash	3702.90
120182	85.12	1/1/2013 8:00 PM	Cash	3789.02
120182	86.13	1/1/2013 8:00 PM	Cash	3876.15
120182	87.14	1/1/2013 8:00 PM	Cash	3964.29
120182	88.15	1/1/2013 8:00 PM	Cash	4053.44
120182	89.16	1/1/2013 8:00 PM	Cash	4143.60
120182	90.17	1/1/2013 8:00 PM	Cash	4234.77
120182	91.18	1/1/2013 8:00 PM	Cash	4326.95
120182	92.19	1/1/2013 8:00 PM	Cash	4420.14
120182	93.20	1/1/2013 8:00 PM	Cash	4514.34
120182	94.21	1/1/2013 8:00 PM	Cash	4609.55
120182	95.22	1/1/2013 8:00 PM	Cash	4705.77
120182	96.23	1/1/2013 8:00 PM	Cash	4802.99
120182	97.24	1/1/2013 8:00 PM	Cash	4901.23
120182	98.25	1/1/2013 8:00 PM	Cash	5000.48
120182	99.26	1/1/2013 8:00 PM	Cash	5100.74
120182	100.27	1/1/2013 8:00 PM	Cash	5202.01
120182	101.28	1/1/2013 8:00 PM	Cash	5304.29
120182	102.29	1/1/2013 8:00 PM	Cash	5407.58
120182	103.30	1/1/2013 8:00 PM	Cash	5511.88
120182	104.31	1/1/2013 8:00 PM	Cash	5617.19
120182	105.32	1/1/2013 8:00 PM	Cash	5723.51
120182	106.33	1/1/2013 8:00 PM	Cash	5830.84
120182	107.34	1/1/2013 8:00 PM	Cash	5939.18
120182	108.35	1/1/2013 8:00 PM	Cash	6048.53
120182	109.36	1/1/2013 8:00 PM	Cash	6158.89
120182	110.37	1/1/2013 8:00 PM	Cash	6270.26
120182	111.38	1/1/2013 8:00 PM	Cash	6382.64
120182	112.39	1/1/2013 8:00 PM	Cash	6496.03
120182	113.40	1/1/2013 8:00 PM	Cash	6610.43
120182	114.41	1/1/2013 8:00 PM	Cash	6725.84
120182	115.42	1/1/2013 8:00 PM	Cash	6842.26
120182	116.43	1/1/2013 8:00 PM	Cash	6959.69
120182	117.44	1/1/2013 8:00 PM	Cash	7078.13
120182	118.45	1/1/2013 8:00 PM	Cash	7197.58
120182	119.46	1/1/2013 8:00 PM	Cash	7318.04
120182	120.47	1/1/2013 8:00 PM	Cash	7439.51
120182	121.48	1/1/2013 8:00 PM	Cash	7561.99
120182	122.49	1/1/2013 8:00 PM	Cash	7685.48
120182	123.50	1/1/2013 8:00 PM	Cash	7809.98
120182	124.51	1/1/2013 8:00 PM	Cash	7935.49
120182	125.52	1/1/2013 8:00 PM	Cash	8061.99
120182	126.53	1/1/2013 8:00 PM	Cash	8189.52
120182	127.54	1/1/2013 8:00 PM	Cash	8318.06
120182	128.55	1/1/2013 8:00 PM	Cash	8447.61
120182	129.56	1/1/2013 8:00 PM	Cash	8578.17
120182	130.57	1/1/2013 8:00 PM	Cash	8709.74
120182	131.58	1/1/2013 8:00 PM	Cash	8842.32
120182	132.59	1/1/2013 8:00 PM	Cash	8975.91
120182	133.60	1/1/2013 8:00 PM	Cash	9110.51
120182	134.61	1/1/2013 8:00 PM	Cash	9246.12
120182	135.62	1/1/2013 8:00 PM	Cash	9382.74
120182	136.63	1/1/2013 8:00 PM	Cash	9520.37
120182	137.64	1/1/2013 8:00 PM	Cash	9659.01
120182	138.65	1/1/2013 8:00 PM	Cash	9798.66
120182	139.66	1/1/2013 8:00 PM	Cash	9939.32
120182	140.67	1/1/2013 8:00 PM	Cash	10080.99
120182	141.68	1/1/2013 8:00 PM	Cash	10223.67
120182	142.69	1/1/2013 8:00 PM	Cash	10367.36
120182	143.70	1/1/2013 8:00 PM	Cash	10512.06
120182	144.71	1/1/2013 8:00 PM	Cash	10657.77
120182	145.72	1/1/2013 8:00 PM	Cash	10804.49
120182	146.73	1/1/2013 8:00 PM	Cash	10952.22
120182	147.74	1/1/2013 8:00 PM	Cash	11100.96
120182	148.75	1/1/2013 8:00 PM	Cash	11250.71
120182	149.76	1/1/2013 8:00 PM	Cash	11401.47
120182	150.77	1/1/2013 8:00 PM	Cash	11553.24
120182	151.78	1/1/2013 8:00 PM	Cash	11706.02
120182	152.79	1/1/2013 8:00 PM	Cash	11859.81
120182	153.80	1/1/2013 8:00 PM	Cash	12014.61
120182	154.81	1/1/2013 8:00 PM	Cash	12170.42
120182	155.82	1/1/2013 8:00 PM	Cash	12327.24
120182	156.83	1/1/2013 8:00 PM	Cash	12485.07
120182	157.84	1/1/2013 8:00 PM	Cash	12643.91
120182	158.85	1/1/2013 8:00 PM	Cash	12803.76
120182	159.86	1/1/2013 8:00 PM	Cash	12964.62
120182	160.87	1/1/2013 8:00 PM	Cash	13126.49
120182	161.88	1/1/2013 8:00 PM	Cash	13289.37
120182	162.89	1/1/2013 8:00 PM	Cash	13453.26
120182	163.90	1/1/2013 8:00 PM	Cash	13618.16
120182	164.91	1/1/2013 8:00 PM	Cash	13784.07
120182	165.92	1/1/2013 8:00 PM	Cash	13950.99
120182	166.93	1/1/2013 8:00 PM	Cash	14118.92
120182	167.94	1/1/2013 8:00 PM	Cash	14287.86
120182	168.95	1/1/2013 8:00 PM	Cash	14457.81
120182	169.96	1/1/2013 8:00 PM	Cash	14628.77
120182	170.97	1/1/2013 8:00 PM	Cash	14799.74
120182	171.98	1/1/2013 8:00 PM	Cash	14971.72
120182	172.99	1/1/2013 8:00 PM	Cash	15144.71
120182	173.00	1/1/2013 8:00 PM	Cash	15318.71
120182	174.01	1/1/2013 8:00 PM	Cash	15493.72
120182	175.02	1/1/2013 8:00 PM	Cash	15669.74
120182	176.03	1/1/2013 8:00 PM	Cash	15846.77
120182	177.04	1/1/2013 8:00 PM	Cash	16024.81
120182	178.05	1/1/2013 8:00 PM	Cash	16203.86
120182	179.06	1/1/2013 8:00 PM	Cash	16383.92
120182	180.07	1/1/2013 8:00 PM	Cash	16564.99
120182	181.08	1/1/2013 8:00 PM	Cash	16747.07
120182	182.09	1/1/2013 8:00 PM	Cash	16929.16
120182	183.10	1/1/2013 8:00 PM	Cash	17112.26
120182	184.11	1/1/2013 8:00 PM	Cash	17296.37
120182	185.12	1/1/2013 8:00 PM	Cash	17481.49
120182	186.13	1/1/2013 8:00 PM	Cash	17667.62
120182	187.14	1/1/2013 8:00 PM	Cash	17854.76
120182	188.15	1/1/2013 8:00 PM	Cash	18042.91
120182	189.16	1/1/2013 8:00 PM	Cash	18232.07
120182	190.17	1/1/2013 8:00 PM	Cash	18422.24
120182	191.18	1/1/2013 8:00 PM	Cash	18613.42
120182	192.19	1/1/2013 8:00 PM	Cash	18805.61
120182	193.20	1/1/2013 8:00 PM	Cash	19000.00
120182	194.21	1/1/2013 8:00 PM	Cash	19195.49
120182	195.22	1/1/2013 8:00 PM	Cash	19392

1 37. The screen shots of the cash sales for January 1, 2013 and January 12, 2013,  
2 are the type of record in style and content we saw when the CI ran the zipper program for us.

3 38. We saw a reply email from Udompanit to Chandillada@hotmail.com  
4 confirming that the zipper was placed in the showticket2013 folder.  
5

6 ***Search Warrant Executed on Bai Tong Emails***

7 39. On July 11, 2017, Microsoft produced several thousand Bai Tong business  
8 emails in response to a federal search warrant. I currently am in the preliminary stages of  
9 reviewing the production and have not yet reviewed all of the emails.

10 40. However, I have noted emails made relevant by prior discussions with CI and  
11 CI 2. CI and CI 2 told us that the SmilePOS system could be programed to send a daily  
12 email with the daily accounting summary of each restaurant. This email summarized total  
13 daily sales, total daily payments in credit cards, and total daily payments in cash, among  
14 other things.

15 41. In my review to date, it appears that the Bai Tong owners enabled this feature  
16 beginning sometime in 2013 and continuing at least until 2016. I have found emails with  
17 daily accounting summaries for each of their operating restaurants. It appears that most  
18 emails have been produced, although there are some days for which I have not yet found  
19 such an email.

20 42. These daily accounting summary emails are probative because we believe,  
21 based on information from CI and CI 2, that the restaurant owners do not operate the time-  
22 consuming SmilePOS Freshbooks program to delete cash sales every night. Rather,  
23 Freshbooks is executed at the end of each month or each quarter - before the IRS and  
24 Washington State DOR periodic reports are filed. Therefore, comparing a tally of the daily  
25 accounting summaries for a specific time period to the numbers submitted in the IRS and  
26 DOR reports for the same time period will reveal whether the Bai Tong restaurants owners  
27 use Freshbooks to skim cash, underreport income, and underpay taxes.  
28

1        43. I have compared the January 2014 Bai Tong Redmond emailed (1) daily cash  
2 payments, (2) daily credit payments, and (3) total sales to the Bai Tong Redmond numbers  
3 reported to DOR in the audit and found the following:

- 4        - The restaurant was closed on January 1, so it was opened for thirty days that month.
- 5        - Twenty eight daily emails were found; I have not located daily emails for two of the  
6 days that month.
- 7        - The emailed daily credit card sales for the twenty eight days were identical to the  
8 daily credit card amounts reported to Washington DOR.
- 9        - Only two days of daily cash sales matched the daily cash sales amounts reported to  
10 Washington DOR.
- 11       - Twenty six days of emailed daily cash sales were higher than the daily cash sales  
12 reported to Washington DOR.
- 13       - Two days of emailed total sales matched the amount reported to Washington DOR.
- 14       - Twenty six days of emailed total sales were higher than the amount reported to  
15 Washington DOR.

16       44. My conclusion is that the January 2014 cash and total sales of Bai Tong  
17 Redmond were underreported to Washington DOR.

18       45. I have confirmed that the 2014 yearly total sales that Bai Tong Redmond  
19 reported to the IRS are nearly the same figures that Bai Tong Redmond reported to  
20 Washington DOR. The difference is less than 0.05%.

21       46. I continue to review the daily accounting summary emails and compare the  
22 numbers contained therein to the numbers Bai Tong Redmond has reported to taxing  
23 authorities. I hope to determine whether this preliminary result is a constant pattern or an  
24 anomaly for this and other Bai Tong Restaurants.

25  
26 **V. PROBABLE CAUSE FOR THE TWO SPECIFIC SEARCH LOCATIONS**

27       There are two locations in this application. One is a house within a residential  
28 Bellevue neighborhood which appears to function as an off-site office for PORNCHAI

1 CHAISEEHA and the BAI TONG Group; the other is the BAI TONG RESTAURANT in  
2 Redmond.

3  
4 **13921 SE 47th Street, Bellevue, Washington 98004**  
5 **House in a Residential Neighborhood - Attachment A1**

6 *Public Information*

7  
8 47. In November 2016, IRS was informed that Bai Tong had moved its offices to a  
9 home in Bellevue, Washington, with the following address: 13921 SE 47<sup>th</sup> Street, Bellevue,  
10 Washington 98006. This information was obtained through a conversation with an employee  
11 at one of the restaurants in the Bai Tong Group.

12 48. I reviewed public records filed with King County Recorder's Office for the  
13 property at 13921 SE 47<sup>th</sup> Street, Bellevue, Washington 98006. The records show that since  
14 August 7, 2015, the property is owned by SFT, LLC. SFT, LLC is a Taiwanese Company.  
15 From the public records I was not able to determine if there is any connection between SFT,  
16 LLC and Bai Tong Restaurants or its owners.

17 49. A search on April 3, 2017 of Lexis Nexis (Law Enforcement Records  
18 Database) shows that 13921 SE 47<sup>th</sup> Street, Bellevue, Washington 98006 as a listed address  
19 for CHADILLADA LAPANGKURA. She was listed as being connected to this address  
20 since August 2016. Lexis Nexis also lists the current Comcast phone line registered to  
21 13921 SE 47<sup>th</sup> Street, Bellevue, Washington 98006 as registered to Thai Bai Tong LLC.

22 *Refuse Examinations*

23  
24 50. On Wednesday, February 1, 2017, I retrieved the refuse and recycling from  
25 13921 SE 47<sup>th</sup> Street, Bellevue, Washington 98006. The refuse and recycling had been left  
26 on the curb of the residence for the weekly trash pick-up. The following relevant items were  
27 recovered from among the trash:  
28



- 1 • Over a hundred “Bai Tong Thai Restaurant” customer comment cards. Each card  
2 rates the restaurant on several attributes and the customers’ contact information is  
3 written on the bottom of the card in order to be placed in a drawing for a \$10 gift card  
4 to “Bai Tong Thai Restaurant.”
- 5 • A loan document titled “Waiver Regarding Appraisal Report” for a property at 20510  
6 Jacklight Lane, Bend, Oregon 97702 (Loan Number XXXXXX0371). The report lists  
7 PORNCHAI CHAISEEHA and CHADILLADA LAPANGKURA as borrowers. It is  
8 signed in blue ink by both PORNCHAI CHAISEEHA and CHADILLADA  
9 LAPANGKURA and dated July 14, 2015.
- 10 • A “Credit Card Authorization Form” for Pinnacle Capital Mortgage (Loan Number  
11 XXXXXX0371). The Card holder’s name PORNCHAI CHAISEEHA, address  
12 21622 95<sup>th</sup> Place South, Kent, Washington 98031, credit card number and expiration  
13 date are written in blue ink on the form. The form is also signed in blue ink by  
14 PORNCHAI CHAISEEHA.

15 51. I looked up the Deschutes County, Oregon Online Public Property Information  
16 for 20510 Jacklight Lane, Bend, Oregon 97702. The public records show that 20510  
17 Jacklight Lane, Bend, Oregon 97702 was last purchased in 2015 by PORNCHAI  
18 CHAISEEHA of 21622 95<sup>th</sup> Place South, Kent, Washington 98031. I obtained the 2013  
19 Form 1040 U.S. Individual Income Tax Return filed with the IRS for PORNCHAI  
20 CHAISEEHA and CHADILLADA LAPANGKURA. The tax return lists 21622 95<sup>th</sup> Place  
21 South, Kent, Washington 98031 as the home address for both parties.

22 52. On Wednesday, July 12, 2017, I retrieved the refuse and recycling from 13921  
23 SE 47<sup>th</sup> Street, Bellevue, Washington 98006. The refuse and recycling had been left on the  
24 curb of the residence for the weekly trash pick-up. The following relevant items were  
25 recovered from the trash:

- 26 • A letter and envelope from Hometown Advisor Real Estate in Bellevue, Washington  
27 to PORNCHAI & CHADILLADA CHAISEEHA at 5590 S. 150th St. Tukwila,  
28 Washington 98188.
- Used airline luggage tags for Jantana Chaiseeha and Rampeepat Chaiseeha.
- An envelope from the King County Records and Licensing Services Division.

1 53. I researched King County Online Public Property Information for 5590 South  
2 150th Street, Tukwila, Washington 98188 and found that public records show that 5590  
3 South 150th Street, Tukwila, Washington 98188 was purchased in 2008, and currently is  
4 owned, by PORNCHAI CHAISEEHA and CHADILLADA LAPANGKURA.

5 54. I know from reviewing public records that Jantana Chaiseeha and Rampeepat  
6 Chaiseeha are family members and part owners in several restaurants in the Bai Tong Group.

7 55. From my training and experience I know business owners and accountants  
8 often keep or take work documents (i.e., financial documents, invoices, bills, payroll  
9 documents, receipts, etc.) to the location where they actually work on the documents. These  
10 work documents may also be sent directly to their home address. Frequently business  
11 owners maintain a home office to work on bills, payroll, accounting, taxes, etc. while at  
12 home and remnants from these documents often are found in the trash from their personal  
13 residence.

14  
15 *Vehicles Parked at 13921 SE 47th Street, Bellevue, Washington 98006*

16 56. On February 24, 2017, at around 9:10 a.m., I drove by 13921 SE 47<sup>th</sup> Street,  
17 Bellevue, Washington 98006. I noticed that the following vehicles were parked in large  
18 driveway on the residence and I have determined the registered owners:

- 19 • 2011 Honda G37 (Washington Plate #AFD2424) - registered owner PORNCHAI  
20 CHAISEEHA d/b/a Bai Tong Family LLC  
21 • 2016 Mazda CX-9 (Washington Plate #BBZ6838) - registered owner Bai Tong  
22 Family LLC  
23 • 2008 Subaru Tri4D (Washington Plate #BBL1029) - registered owner Unchisa  
24 Sanpavat  
25 • 2001 Honda Accord (Washington Plate #BBA1131) - registered owner Karn  
26 Kanpittaya

27 57. On March 1, 2017, at around 10:05 a.m. I drove by 13921 SE 47<sup>th</sup> Street,  
28 Bellevue, Washington 98006. I noticed that the following vehicles were parked in large  
driveway on the residence and I determined the registered owners:

- 2011 Honda G37 (Washington Plate #AFD2424) - registered OWNER PORNCCHAI CHAISEEHA d/b/a Bai Tong Family LLC
- 2016 Mazda CX-9 (Washington Plate #BBZ6838) - registered owner Bai Tong Family LLC
- 2008 Subaru Tri4D (Washington Plate #BBL1029) - registered owner Unchisa Sanpavat
- 2001 Honda Accord (Washington Plate #BBA1131) - registered owner Karn Kanpittaya

58. On March 13, 2017, at around 09:20 a.m. I drove by 13921 SE 47<sup>th</sup> Street, Bellevue, Washington 98006. I noticed that the following vehicles were parked in large driveway on the residence and I determined the registered owners:

- 2016 Mazda CX-9 (Washington Plate# BBZ6838) - registered owner Bai Tong Family LLC
- 2001 Honda Accord (Washington Plate# BBA1131) - registered owner Karn Kanpittaya
- V2016 VW Golf (Washington Plate# AXD6107) - registered owner Criss-Cross Applesauce Corp, PORNCCHAI CHAISEEHA
- 2014 Acura MDX (Washington Plate# AON2682) - registered owner Bai Tong Family LLC, PORNCCHAI CHAISEEHA

59. In this investigation I have reviewed Washington Secretary of State Online Corporate Filings which show that PORNCCHAI CHAISEEHA and CHADILLADA LAPANGKURA are the registered agents and governing persons for Criss-Cross Applesauce Incorporated.

60. On March 22, 2017, at around 09:10 a.m. I drove by 13921 SE 47<sup>th</sup> Street, Bellevue, Washington 98006. I noticed that the following vehicles were parked in large driveway on the residence and I determined the registered owners:

- 2011 Honda G37 (Washington Plate# AFD2424) - registered owner PORNCCHAI CHAISEEHA d/b/a Bai Tong Family LLC
- 2008 Subaru Tri4D (Washington Plate# BBL1029) - registered owner Unchisa Sanpavat

- 2014 Acura MDX (Washington Plate# AON2682) - registered owner Bai Tong Family LLC, PORNCHAI CHAISEEHA
- V2016 VW Golf (Washington Plate# AXD6107) - registered owner Criss-Cross Applesauce Corp, PORNCHAI CHAISEEHA

61. I reviewed the records from the Washington Department of Licensing Online Database and found that Karn Kanpittaya has registered 13921 SE 47th Street, Bellevue, Washington as his primary address. I reviewed facebook and found the page of someone with the name Karn Kanpittaya who lived in Bellevue and who was facebook friends with CHADILLADA LAPANGURA. There was no additional relevant information on facebook and I have not found any additional public information on Karn Kanpittaya.

62. I reviewed the records from the Washington Department of Licensing and noted that Unchisa Sanpavat has registered 5590 South 150th Street, Tukwila, Washington as her primary address. I looked up the King County Online Public Property Information for 5590 South 150th Street, Tukwila, Washington 98188. The public records show that 5590 South 150th Street, Tukwila, Washington 98188 was purchased in 2008, and currently is owned, by PORNCHAI CHAISEEHA and CHADILLADA LAPANGKURA.

63. I also reviewed IRS & Washington DOR payroll records for Unchisa Sanpavat and from the years 2012 to 2016 she worked as an employee for several different business including the following Bai Tong Group businesses:

- Bai Tong Thai Corporation
- Bai Tong Family LLC.
- Noi Downtown Seattle LLC
- Noi Issaquah LLC
- Noi LLC
- Criss-Cross Applesauce Inc.

*Mail Sent to 13921 SE 47th Street, Bellevue, Washington 98006*

64. During April 2017, mail and packages were sent to 13921 SE 47<sup>th</sup> Street, Bellevue, Washington 98006 which were addressed to CHADILLA LAPANGKURA and/or

1 PORNCHAI CHAISEEHA and/or BAI TONG. There were also mail items addressed to  
2 other unknown parties. The mail addressed to CHADILLA LAPANGKURA and/or  
3 PORNCHAI CHAISEEHA and/or BAI TONG included pieces from the following return  
4 addressees:

- 5 • Amazon Distribution
- 6 • City of Bellevue
- 7 • AT&T
- 8 • Comcast
- 9 • American Express
- Puget Sound Energy

10 65. From my training and experience I know businesses often have financial  
11 documents (i.e., Bank Statements, Invoices, Supplier and Customer Invoices, Tax  
12 Documents, etc.) sent to the location which is used as a business office and where the  
13 financial documents are reviewed, accounted for, and filed for record keeping purposes.  
14

15 **14804 NE 24th St. Redmond, Washington 98052**  
16 **Restaurant in a Shopping District – Attachment A2**

17 *Public Information*  
18

19 66. I reviewed the Washington Secretary of State website which lists the  
20 businesses registered in the state of Washington. The website noted that Bai Tong Family,  
21 LLC has been legally registered as a Limited Liability Corporation since 2009 and remains  
22 registered as such. The Registered Agent for the business is PORNCHAI CHAISEEHA and  
23 the address listed is 14804 NE 24th St. Redmond, Washington 98052.

24 67. I reviewed the Washington Department of Revenue website which lists the  
25 businesses registered in the state of Washington. The website noted that Bai Tong Family,  
26 LLC, using the business name *Bai Tong Thai Restaurant*, has been legally registered as a  
27 Limited Liability Corporation since 2010 and remains registered as such. The business is  
28

1 classified as a full service restaurant. Both the Mailing and Business address for the Bai  
2 Tong Thai is 14804 NE 24th St. Redmond, Washington 98052.

3 68. I reviewed the website www.baitongrestaurant.com. This is the official website  
4 for the multiple Bai Tong Restaurants. Under locations tab on the website the Redmond  
5 location is listed at the following address: 14804 NE 24th St. Redmond, Washington  
6 98052.

7  
8 *Federal Tax Returns*

9 69. I reviewed the 2011 to 2014 Forms 1065, U.S. Federal Return of Partnership  
10 Income, for *Bai Tong Family LLC* that were submitted to the IRS. The address listed on  
11 each of these tax returns was 14804 NE 24th St. Redmond, Washington 98052. Each of the  
12 tax returns was signed by PORNCHAI CHAISEEHA.

13  
14 *Observations*

15 70. On Monday, June 26, 2017, I went into Bai Tong Thai Restaurant at 14804 NE  
16 24th St. Redmond, Washington 98052 at approximately 12:00 pm. The restaurant was busy  
17 and it appeared that most of the tables were full of customers. There were several people in  
18 the front of the restaurant waiting to be seated. I was in a party of three and had to wait 20  
19 minutes to be seated.

20 71. On the way to our table, I walked through the restaurant to my table. I noticed  
21 several POS terminals around the restaurant. I watched as servers entered orders into the  
22 terminals and processed payments. I was able to observe the screen of the terminals close  
23 enough to notice SmilePOS's name and logo was in the corner of the screen.

24 72. At the end of my meal I obtained a receipt for my lunch purchase (and my two  
25 co-workers dining with me):  
26  
27  
28



Date: 6/26/2017 12:42 PM Table #4  
Server: Emey (T.1)  
( L ) Phad Soi-Lew \$9.50  
Total 1 item(s) \$9.50  
Sales Tax \$0.95  
Grand Total \$10.45  
Paid by Cash \$15.00  
Change \$4.55

18% Gratuity Included for a party of 6 people or more.  
Thank you. Please Come Again.

- RECEIPT -

Date: 6/26/2017 12:42 PM Table #4  
Server: Emey (T.2)  
Diet Coke \$2.95  
Roast Duck Curry \$21.95  
Total 2 item(s) \$24.90  
Sales Tax \$2.49  
Grand Total \$27.39  
Paid by Cash \$40.00  
Change \$12.61

18% Gratuity included for a party of 6 people or more.  
Thank you. Please Come Again.

- RECEIPT -

Date: 6/26/2017 12:42 PM Table #4  
Server: Emey (T.3)  
( L ) Cashew Chicken \$10.50  
Total 1 item(s) \$10.50  
Sales Tax \$1.05  
Grand Total \$11.55  
Paid by Cash \$15.00  
Change \$3.45

18% Gratuity included for a party of 6 people or more.  
Thank you. Please Come Again.

- RECEIPT -

73. I noticed that the style of the receipt that I received is the same style of receipt that DOR received when it was conducting its audit of *Bai Tong Thai Restaurant* in Redmond. I could tell from the style of receipt that it was printed from a SmilePOS system. Based on my review of the screens in the restaurant and the receipt I received it appears that *Bai Tong Thai Restaurant* in Redmond, Washington is still using SmilePOS software on site.

From my training and experience I know businesses often keep business and accounting and financial records at the location where business is conducted. Restaurants often keep track of revenue, expenses and cash at the location of the business to make sure that accounting records are accurately recorded.

## VI. ITEMS TO BE SEARCHED AND SEIZED

### Items believed to be located at Search Locations

I believe there will be evidence of the above-described crimes at the location listed above because individuals who attempt to conceal their true income, or who help others conceal their true income, the true income of companies they control, and the true ownership of their assets, will keep notes and correspondence, will maintain books and records of their financial activity, such as receipts for expenditures by cash and check and credit and debit cards, money orders and cashier's checks, bank records, loan documents evidencing the

1 obtaining, secreting, transfer, or concealment of assets and the obtaining, secreting, transfer,  
2 concealment and expenditure of money, personal tax returns with supporting documentation,  
3 notes with names, business identification numbers and/or social security numbers, account  
4 information, and other financial documents at their place of residence and their place of  
5 business, where they have ready access to these documents.

6 Based upon my training, experience and participation in this and other financial  
7 investigations involving criminal tax violations and conspiracy to defraud the government,  
8 and based upon my conversations with other experienced special agents who have  
9 participated in similar investigations, I know:

- 10 - that businesses typically retain accounting books and records at their business  
11 location and/or personal residence;
- 12 - that such books and records are made in an attempt to trace or track the flow of  
13 funds into and out of the business, to and from owners, investors, lenders,  
14 suppliers, customers and others;
- 15 - that such books and records are used as the basis for the preparation of  
16 financial statements and also for the preparation of tax returns due to federal, state, and local  
17 taxing authorities;
- 18 - that such books and records are ordinarily kept and retained at the  
19 place of business for extended periods of time, often several years, for a number of reasons,  
20 one of which is to provide documentation and evidence in support of shareholder and partner  
21 basis or investment, asset liability, revenue and expense transactions if questioned by IRS  
22 auditors, or other taxing authorities;
- 23 - that individuals who attempt to conceal their true income, and who help  
24 others conceal their true income, the true income of companies they control and the true  
25 ownership of assets often retain at their business location, and at their personal residence,  
26 records with false entries, such as nominee names, altered dates, altered amounts, altered  
27 classifications and altered descriptions of business transactions;
- 28 - that individuals who attempt to conceal their true income, and who help



1 others conceal their true income, the true income of the companies they control and true  
2 ownership of assets retain at their business location, and at their personal residence, secret  
3 bank, brokerage, and other financial institution account records, in some cases both foreign  
4 and domestic, that document the flow of funds into and out of the business;

5 - that individuals who attempt to conceal their true income, and who  
6 help others conceal their true income, the true income of companies they control and the true  
7 ownership of assets often retain at their business location, and at their personal residence, a  
8 separate set of accounting records that document sources of income not reported to taxing  
9 authorities;

10 - that individuals who attempt to conceal their true income, and who help  
11 others conceal their true income, the true income of companies they control and the true  
12 ownership of assets often retain at their business location, and at their personal residence,  
13 records relating to the identity of undisclosed principals and related party transactions;

14 - that individuals who attempt to conceal their true income, and who and  
15 help others conceal their true income, the true income of companies they control and the true  
16 ownership of assets often retain at their business location, and at their personal residence,  
17 books and records evidencing the obtaining, secreting, transfer or concealment of assets and  
18 the obtaining, secreting, transfer, concealment and expenditure of money, where that  
19 individual has ready access to these documents; and

20 - that individuals who file personal income and business or partnership income tax  
21 returns will often maintain copies of those returns, along with supporting work  
22 papers and other documentation relating to those returns.

23 - that individuals who own or benefit from cash intensive businesses that  
24 commit tax evasion or conspiracy of tax evasion often hide cash from the government by not  
25 depositing it in the bank and/or by structuring the deposits and withdrawals, that is,  
26 depositing cash in amounts less than \$10,000. They often keep cash hoards in safes or at  
27 other locations at home or business. They often make business and personal purchases with  
28

1 cash, rather than using credit cards or checks, as the cash has not been deposited in the bank  
2 and therefore is not recorded by a third-party record.  
3

#### 4 **Computers, Electronic Storage, and Forensic Analysis**

5 Records of the type described in the preceding paragraphs are also often stored on  
6 digital devices.

7 Persons engaged in fraudulent tax schemes often maintain such records for long  
8 periods of time, particularly when they are involved in ongoing criminal conduct. There are  
9 many reasons why criminal offenders maintain evidence for lengthy periods of time. The  
10 evidence may appear innocuous at first glance (e.g. financial, credit card and banking  
11 documents, travel documents, receipts, documents reflecting purchases of assets, personal  
12 calendars, telephone and address directories, check books, videotapes and photographs,  
13 utility records, ownership records, letters and note, tax returns and financial records, escrow  
14 files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware  
15 and software), but have significance and relevance when considered together and in light of  
16 other evidence. The criminal offender may no longer realize he or she still possesses the  
17 evidence, or may believe that law enforcement would not be able to obtain a warrant to seize  
18 the evidence. The criminal offender may also be under the mistaken belief that he or she has  
19 deleted, hidden, or otherwise destroyed computer-related evidence, but which evidence may  
20 yet be retrievable by a trained forensic computer expert.

21 As described above and in Attachment B, this application seeks permission to search  
22 for evidence, fruits and/or instrumentalities that might be found at the search locations  
23 described in Attachments A1 and A2, in whatever form they are found. One form in which  
24 the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices  
25 such as computer hard drives or other electronic storage media.<sup>2</sup>  
26  
27

28 <sup>2</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded.  
Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 Thus, the warrant applied for would authorize the seizure of digital devices or other  
2 electronic storage media or, possibly, the copying of electronically stored information from  
3 digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

4  
5 ***Probable Cause***

6 Based upon my review of the evidence gathered in this investigation, my review of  
7 data and records, information received from other agents and computer forensics examiners,  
8 and my training and experience, I submit that if a digital device or other electronic storage  
9 media is found at the search locations described in Attachments A1 and A2, there is probable  
10 cause to believe that evidence, fruits, and/or instrumentalities of the crimes of Conspiracy to  
11 Commit Tax Evasion and to defraud the United States, in violation of 18 U.S.C. § 371, will  
12 be stored on those digital devices or other electronic storage media.

13 The evidence collected to date establishes probable cause to believe that digital  
14 devices or other electronic storage are being used or have been used during the course of the  
15 underlying scheme, to, among other things:

- 16 - create and store documents representing purchases and sales of PORNCHAI  
17 CHAISEEHA and CHADILLADA LAPANGKURA or their businesses<sup>3</sup>;  
18 - create and store documents representing income and expenses for PORNCHAI  
19 CHAISEEHA and CHADILLADA LAPANGKURA or their businesses;  
20 - create and store software that is used to suppress sales (zapper or tax evading  
21 software);

22 There is, therefore, probable cause to believe that evidence, fruits and instrumentalities of the  
23 crimes of 18 U.S.C. § 371 (conspiracy to commit tax evasion); will be found on digital  
24 devices or other electronic storage media at the search locations in Attachments A1 and A2,  
25 for the following reasons:

26  
27 <sup>3</sup> For the purpose of this Search Warrant, PORNCHAI CHAISEEHA and CHADILLADA  
28 LAPANGKURA and their businesses shall be: Bai Tong Restaurant LLC, Bai Tong Family LLC, BT Capitol Hill  
LLC, Bai Tong Thai Corporation, Noi LLC, Noi Downtown Seattle LLC, Noi Hawaii LLC, and Isarn Soul Food LLC.

1 Based on my knowledge, training, and experience, I know that computer files or  
2 remnants of such files can be recovered months or even years after they have been  
3 downloaded onto a digital device or other electronic storage medium, deleted, or viewed via  
4 the Internet. Electronic files downloaded to a digital device or other electronic storage  
5 medium can be stored for years at little or no cost. Even when files have been deleted, they  
6 can be recovered months or years later using forensic tools. This is so because when a person  
7 "deletes" a file on a digital device or other electronic storage media, the data contained in the  
8 file does not actually disappear; rather, that data remains on the storage medium until it is  
9 overwritten by new data.

10 Therefore, deleted files, or remnants of deleted files, may reside in free space or slack  
11 space-that is, in space on the digital device or other electronic storage medium that is not  
12 currently being used by an active file-for long periods of time before they are overwritten. In  
13 addition, a computer's operating system may also keep a record of deleted data in a "swap"  
14 or "recovery" file.

15 Wholly apart from user-generated files, computer storage media, in particular,  
16 computers' internal hard drives, contain electronic evidence of how a computer has been  
17 used, what it has been used for, and who has used it. To give a few examples, this forensic  
18 evidence can take the form of operating system configurations, artifacts from operating  
19 systems or application operations, file system data structures, and virtual memory "swap" or  
20 paging files. Computer users typically do not erase or delete this evidence, because special  
21 software is typically required for that task. However, it is technically possible to delete this  
22 information.

23 Similarly, files that have been viewed via the Internet are sometimes automatically  
24 downloaded into a temporary Internet directory or "cache."

25 Based on interviews conducted during the course of this investigation with related  
26 parties, I believe that digital devices and other electronic storage media were used to  
27 generate, store, and print documents used in offenses executed by PORNCHAI  
28 CHAISEEHA and CHADILLADA LAPANGKURA and their businesses, that is,

1 Conspiracy to Commit Tax Evasion and to Defraud the Government, in violation of Title 18,  
2 United States Code, § 371.

3 Based on the scope of the investigation, I believe it is likely that PORNCCHAI  
4 CHAISEEHA and CHADILLADA LAPANGKURA will continue to have some records  
5 related to the underlying scheme and the proceeds generated by the scheme in both paper and  
6 electronic formats. This is because a scheme of this scope requires substantial records to  
7 keep track of the various aspects, including purchases, sales, profits, and expenses.  
8 Criminals, even when fully aware of ongoing investigations, frequently keep these records  
9 for long periods of time. Especially sensitive records may be maintained in electronic  
10 storage devices such as hidden thumb drives or other portable media, including smart phones  
11 and other more easily concealed devices. Likewise, with regard to any personal computers  
12 found at the residence or automobiles, evidence of PORNCCHAI CHAISEEHA and  
13 CHADILLADA LAPANGKURA business and financial life -- including money spent on  
14 business, everyday goods, travel, restaurants, investments, gifts, house repairs, electronics,  
15 automobiles, and real estate, to give just some examples -- would be relevant to the  
16 investigation for tax evasion. Therefore, I believe there is reason to believe that digital  
17 devices or electronic storage media currently located at the Search Locations may contain  
18 some or all of the items to be seized in Attachment B.

19  
20 ***Forensic Evidence***

21 As further described in Attachment B, this application seeks permission to locate not  
22 only computer files that might serve as direct evidence of the crimes described on the  
23 warrant, but also for forensic electronic evidence that establishes how digital devices or other  
24 electronic storage media were used, the purpose of their use, who used them, and when.  
25 There is probable cause to believe that this forensic electronic evidence will be on any digital  
26 devices or other electronic storage media located at the search locations for the following  
27 reasons:  
28

1        Stored data can provide evidence of a file that was once on the digital device or other  
2 electronic storage media but has since been deleted or edited, or of a deleted portion of a file,  
3 such as a paragraph that has been deleted from a word processing file. Virtual memory  
4 paging systems can leave traces of information on the digital device or other electronic  
5 storage media that show what tasks and processes were recently active. Web browsers, e-  
6 mail programs, and chat programs store configuration information that can reveal  
7 information such as online nicknames and passwords. Operating systems can record  
8 additional information, such as the history of connections to other computers, the attachment  
9 of peripherals, the attachment of USB flash storage devices or other external storage media,  
10 and the times the digital device or other electronic storage media was in use. Computer file  
11 systems can record information about the dates files were created and the sequence in which  
12 they were created.

13        Forensic evidence on a digital device or other electronic storage media can also  
14 indicate who has used or controlled the device. This “user attribution” evidence is analogous  
15 to the search for “indicia of occupancy” while executing a search warrant at a residence. For  
16 example, registry information, configuration files, user profiles, e-mail, e-mail address  
17 books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and  
18 correspondence, and the data associated with the foregoing, such as file creation and last-  
19 accessed dates may all be evidence of who used or controlled the digital device or other  
20 electronic storage media at a relevant time.

21        A person with appropriate familiarity with how a digital device or other electronic  
22 storage media works can, after examining this forensic evidence in its proper context, draw  
23 conclusions about how the digital device or other electronic storage media were used, the  
24 purpose of their use, who used them, and when.

25        The process of identifying the exact files, blocks, registry entries, logs, or other forms  
26 of forensic evidence on a digital device or other electronic storage media that are necessary  
27 to draw an accurate conclusion is a dynamic process. While it is possible to specify in  
28 advance the records to be sought, digital evidence is not always data that can be merely

1 reviewed by a review team and passed along to investigators. Whether data stored on a  
2 computer is evidence may depend on other information stored on the computer and the  
3 application of knowledge about how a computer behaves. Therefore, contextual information  
4 necessary to understand other evidence also falls within the scope of the warrant.

5 Further, in finding evidence of how a digital device or other electronic storage media  
6 was used, the purpose of its use, who used it, and when, sometimes it is necessary to  
7 establish that a particular thing is not present. For example, the presence or absence of  
8 counter-forensic programs or anti-virus programs and associated data may be relevant to  
9 establishing the user's intent.

#### 10 11 **Digital Devices as Instrumentalities of the Crimes**

12 I know that when an individual uses either a business or personal computer in keeping  
13 records the individual's personal computers often will serve both as instrumentalities for  
14 committing the crime and storage media for evidence of the crime. Based on the information  
15 in this Affidavit, I believe that the digital devices at the search locations described in  
16 Attachments A1 and A2 are instrumentalities of crime as well as storage devices, because  
17 they constitute the means by which PORNCHEI CHAISEEHA and CHADILLADA  
18 LAPANGKURA committed the violations. Any personal computers at the search locations  
19 likely were used to commit the crime of conspiracy because they were used by PORNCHEI  
20 CHAISEEHA and/or CHADILLADA LAPANGKURA and their businesses (a) to keep  
21 financial records of profits and receipts from business; (b) contacts to clients that purchased  
22 the tax evading software; (c) to discuss his crimes with co-conspirators others through email  
23 and other communications. Therefore, I believe that in addition to seizing the digital  
24 devices to conduct a search of their contents as set forth herein, there is probable cause to  
25 seize those digital devices as instrumentalities of the criminal activity.

26 If, after conducting its examination, law enforcement personnel determine that any  
27 digital device is any instrumentality of the criminal offenses referenced above, the  
28 government may retain that device during the pendency of the case as necessary to, among

1 other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and  
2 litigate the issue of forfeiture. If law enforcement personnel determine that a device was not  
3 an instrumentality of the criminal offenses referenced above, it shall be returned to the  
4 person/entity from whom it was seized within 90 days of the issuance of the warrant, unless  
5 the government seeks and obtains authorization from the Court for its retention.

#### 6 7 **Past Efforts to Obtain Electronically Stored Information**

8 As part of our investigation, we have executed a search warrant on Google Cloud  
9 Storage and Microsoft for certain files of PORNCHAI CHAISEEHA and CHADILLADA  
10 LAPANGKURA and their businesses. Many of the files that have been received are in Thai  
11 and other records are still waiting to be received. Although I have not been able to read  
12 many of those files yet and I expect some of the email content may be on his home or office  
13 digital devices, most of the content requested in this search warrant should differ  
14 substantially from what was obtained the Google and Microsoft warrant. I have not made  
15 any prior efforts to obtain the evidence based on the consent of any party who may have  
16 authority to consent. Specifically, I believe that if PORNCHAI CHAISEEHA and  
17 CHADILLADA LAPANGKURA, or others who may be involved in the above-described  
18 criminal activity, become aware of the investigation in advance of the execution of a search  
19 warrant, he may attempt to destroy any potential evidence, whether digital or non-digital,  
20 thereby hindering law enforcement agents from the furtherance of the criminal investigation.

#### 21 22 **Risk of Destruction of Evidence**

23 I know, based on my training and experience, that digital information can be very  
24 fragile and easily destroyed. Digital information can also be easily encrypted or obfuscated  
25 such that review of the evidence would be extremely difficult, and in some cases impossible.  
26 I do not know whether in the instant case, PORNCHAI CHAISEEHA and CHADILLADA  
27 LAPANGKURA or others to whom they may have entrusted their records, used encryption  
28 on the computer systems they utilizes to engage in their crimes. If an encrypted computer is



1 either powered off, or if the user has not entered the encryption password and logged onto  
2 the computer, it is likely that any information contained on the computer will be impossible  
3 to decipher. If the computer is powered on, however, and the user is already logged onto the  
4 computer, there is a much greater chance that the digital information can be extracted from  
5 the computer. This is because when the computer is on and in use, the password has already  
6 been entered and the data on the computer is accessible. However, giving the owner of the  
7 computer time to activate a digital security measure, pull the power cord from the computer,  
8 or even log off of the computer, could result in a loss of digital information that could  
9 otherwise have been extracted from the computer.

#### 11 **Request for Authority to Conduct Off-Site Search of Target Computers**

##### 12 ***Necessity of Seizing or Copying Entire Computers or Storage Media.***

13 In most cases, a thorough search of premises for information that might be stored on  
14 digital devices or other electronic storage media often requires the seizure of the physical  
15 items and later off-site review consistent with the warrant. In lieu of removing all of these  
16 items from the premises, it is sometimes possible to make an image copy of the data on the  
17 digital devices or other electronic storage media, onsite. Generally speaking, imaging is the  
18 taking of a complete electronic picture of the device's data, including all hidden sectors and  
19 deleted files. Either seizure or imaging is often necessary to ensure the accuracy and  
20 completeness of data recorded on the item, and to prevent the loss of the data either from  
21 accidental or intentional destruction. This is true because of the following:

22 The time required for an examination. As noted above, not all evidence takes the  
23 form of documents and files that can be easily viewed on site. Analyzing evidence of how a  
24 computer has been used, what it has been used for, and who has used it requires considerable  
25 time, and taking that much time on premises could be unreasonable. As explained above,  
26 because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will  
27 be necessary to thoroughly examine the respective digital device and/or electronic storage  
28 media to obtain evidence. Computer hard drives, digital devices and electronic storage

1 media can store a large volume of information. Reviewing that information for things  
2 described in the warrant can take weeks or months, depending on the volume of data stored,  
3 and would be impractical and invasive to attempt on-site.

#### 4 ***Technical Requirements***

5 Digital devices or other electronic storage media can be configured in several  
6 different ways, featuring a variety of different operating systems, application software, and  
7 configurations. Therefore, searching them sometimes requires tools or knowledge that might  
8 not be present on the search site. The vast array of computer hardware and software  
9 available makes it difficult to know before a search what tools or knowledge will be required  
10 to analyze the system and its data on the premises. However, taking the items off-site and  
11 reviewing them in a controlled environment will allow examination with the proper tools and  
12 knowledge.

#### 13 ***Variety of Forms of Electronic Media***

14 Records sought under this warrant could be stored in a variety of electronic storage  
15 media formats and on a variety of digital devices that may require off-site reviewing with  
16 specialized forensic tools.

#### 18 **Search Techniques**

19 Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of  
20 Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise  
21 copying digital devices or other electronic storage media that reasonably appear capable of  
22 containing some or all of the data or items that fall within the scope of Attachment B to this  
23 Affidavit, and will specifically authorize a later review of the media or information  
24 consistent with the warrant.

25 At this time, I believe that PORNCHEI CHAISEEHA and CHADILLADA  
26 LAPANGKURA work at 13921 SE 47th Street, Bellevue, Washington 98006 (residential  
27 location) and 14804 NE 24th St. Redmond, Washington 98052 (business location).  
28 Additionally, PORNCHEI CHAISEEHA and CHADILLADA LAPANGKURA may reside

1 or intermittently stay at the Bellevue residence. It is also possible that other people share this  
2 search location and it is possible that the search locations described in Attachments A1 and  
3 A2 will contain digital devices or other electronic storage media that are predominantly used,  
4 and perhaps owned, by persons who are not suspected of a crime. If agents conducting the  
5 search nonetheless determine that it is possible that the things described in this warrant could  
6 be found on those computers or digital devices, this application seeks permission to search  
7 and if necessary to seize those computers and digital devices as well. It may be impossible to  
8 determine, on scene, which computers contain the things described in this warrant.

9 Consistent with the above, I am requesting the authority to seize and/or obtain a  
10 forensic image of digital devices or other electronic storage media that reasonably appear  
11 capable of containing data or items that fall within the scope of Attachment B to this  
12 Affidavit, and to conduct off-site searches of the digital devices or other electronic storage  
13 media and/or forensic images, using the following procedures:

14  
15 ***Securing the Data***

16 Upon securing the physical search site, the search team will conduct an initial review  
17 of any digital devices or other electronic storage media located at the subject premises  
18 described in Attachments A1 and A2 that are capable of containing data or items that fall  
19 within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the  
20 data contained on these devices onsite in a reasonable amount of time and without  
21 jeopardizing the ability to accurately preserve the data.

22 In order to examine the electronically stored information ("ESI") in a forensically  
23 sound manner, law enforcement personnel with appropriate expertise will attempt to produce  
24 a complete forensic image, if possible and appropriate, of any digital device or other  
25 electronic storage media that is capable of containing data or items that fall within the scope  
26 of Attachment B to this Affidavit.

27 A forensic image may be created of either a physical drive or a logical drive. A  
28 physical drive is the actual physical hard drive that may be found in a typical computer.

1 When law enforcement creates a forensic image of a physical drive, the image will contain  
2 every bit and byte on the physical drive. A logical drive, also known as a partition, is a  
3 dedicated area on a physical drive that may have a drive letter assigned (for example the c:  
4 and d: drives on a computer that actually contains only one physical hard drive). Therefore,  
5 creating an image of a logical drive does not include every bit and byte on the physical drive.  
6 Law enforcement will only create an image of physical or logical drives physically present  
7 on or within the subject device. Creating an image of the devices located at the search  
8 locations described in Attachments A1 and A2 will not result in access to any data physically  
9 located elsewhere. However, digital devices or other electronic storage media at the search  
10 locations described in Attachments A1 and A2 that have previously connected to devices at  
11 other locations may contain data from those other locations.  
12 In addition to creating an image of a physical or logical drive from a digital device or other  
13 electronic storage media, law enforcement may attempt to create an image of the random  
14 access memory (RAM) of a digital device. Agents may only create an image of a digital  
15 device's RAM if the computer is powered on at the time of the search. This is because RAM  
16 is only active when the device is in operation. Any data contained in the RAM will be lost  
17 when the computer is powered off. A computer's RAM may contain evidence related to who  
18 else is logged onto the computer (even remotely), open connections that might indicate a  
19 program is waiting for commands, passwords for encryption programs, hardware and  
20 software settings, maps of recent files and applications accessed, and information related to  
21 what communication vendors have recently been utilized on the device (i.e. instant  
22 messaging services, e-mail services, social networking sites, etc.). In addition, RAM may  
23 contain encryption keys necessary to access other elements of the subject device.

24 If based on their training and experience, and the resources available to them at the  
25 search site, the search team determines it is not practical to make an on-site image within a  
26 reasonable amount of time and without jeopardizing the ability to accurately preserve the  
27 data, then the digital devices or other electronic storage media will be seized and transported  
28 to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

1        ***Searching the Forensic Images***

2        Searching the forensic images for the items described in Attachment B may require a  
3 range of data analysis techniques. In some cases, it is possible for agents and analysts to  
4 conduct carefully targeted searches that can locate evidence without requiring a time-  
5 consuming manual search through unrelated materials that may be commingled with  
6 criminal evidence. In other cases, however, such techniques may not yield the evidence  
7 described in the warrant, and law enforcement may need to conduct more extensive searches  
8 to locate evidence that falls within the scope of the warrant. The search techniques that will  
9 be used will be only those methodologies, techniques and protocols as may reasonably be  
10 expected to find, identify, segregate and/or duplicate the items authorized to be seized  
11 pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily  
12 expose many or all parts of a hard drive to human inspection in order to determine whether it  
13 contains evidence described by the warrant.

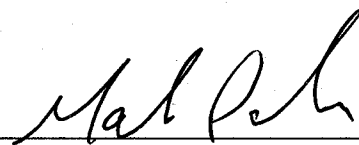
14 These methodologies, techniques and protocols may include the use of a "hash value" library  
15 to exclude normal operating system files that do not need to be further searched. Agents  
16 may utilize hash values to exclude certain known files, such as the operating system and  
17 other routine software, from the search results. However, because the evidence I am seeking  
18 does not have particular known hash values, agents will not be able to use any type of hash  
19 value library to locate the items identified in Attachment B.

20 //

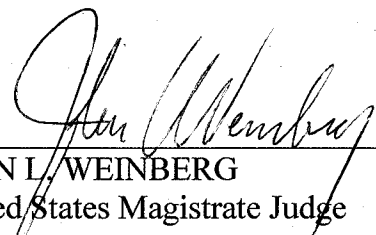
21 //

1 VII. CONCLUSION

2 Based on my experience and the facts set forth in this Affidavit, I believe there is  
3 probable cause to believe documents and records, which are evidence, fruits, and  
4 instrumentalities of violations of Conspiracy to Commit Tax Evasion and to Defraud the  
5 Government in violation of 18 U.S.C. § 371 are maintained at (1) 13921 SE 47th Street,  
6 Bellevue, Washington 98004, described with particularity in Attachment A1, and (2) 14804  
7 NE 24th St. Redmond, Washington 98052 described with particularity in Attachment A2.

8  
9  
10  
11   
12 MARK PAHNKE, Affiant  
13 Special Agent, Internal Revenue Service  
14

15 SUBSCRIBED and SWORN to before me this 2 day of August, 2017.

16  
17   
18 JOHN L. WEINBERG  
19 United States Magistrate Judge  
20  
21  
22  
23  
24  
25  
26  
27  
28